Analysis on Blockchain Mining

1st Md Kamruzzaman
School of EECS
Washington State University
Pullman, USA
methun@eecs.wsu.edu
11481693

2nd Jin Tao
School of EECS
Washington State University
Pullman, USA
jtao@eecs.wsu.edu
11474660

3rd Xiaoqin Fu
School of EECS
Washington State University
Pullman, USA
xiaoqin.fu@wsu.edu
11583773

***Abstract*—The innovation of high computing processors and the availability of high speed Internet help to create a new form of currency named cryptocurrency. One of the most popular digital currencies is Bitcoin. In order to maintain the integrity and secrecy of a transaction between senders and receivers, Bitcoin technology uses the Blockchain technique. Blockchain is a public distributed ledger, which uses either proof–of–work or proof–of–stake procedure to validate a transaction. The process (proof–of–work) to validate a transaction is economically costly and computationally time–consuming process using Turing designed computing machineries. This hardness enforces security. This security can be compromised using an unimaginably powerful computing machine such as the quantum computer. Tangle, which is an advanced quantum secure mechanism that initiates new cryptocurrency called IOTA, is also analyzed.**

***Index Terms*—cryptography, cryptocurrency, bitcoin, blockchain, proof–of–work, proof–of–stake, network, security, tangle, iota**

I. Introduction

Currency is the most ancient form of medium which is used to exchange products and goods. Real currency is easy to maintain and hard to increase without gaining it from any source of income. Virtual currency is an alternative form of real currency, which is the product of modern technology. But virtual currency is hard to maintain and easy to replicate without gaining it from any source. In order to make the nature of the virtual currency similar to real currency, at first, Satoshi Nakamoto proposed a method using block-chain and named it Bitcoin, which was the earliest cryptocurrency.

Bitcoin is one of the cryptocurrencies which deliberately use blockchain technology. Blockchain is a distributed database which keeps records in a distributed fashion. Each block encrypts the data using cryptographic hash function, for instance, SHA-256. Figure 1 shows the schematic diagram of blockchain. A block also keeps record of the next available block so that we can traverse the blocks. A block stores many records in a tree structure where the leaves of the tree store the transaction information and other intermediate nodes store the hash values. The root of this tree belongs to a block which also contains the hash value generated from child nodes. The timestamp in a block is used to synchronize the position of a block in blockchain. A block also contains NONCE value, which is a random unique number for a specific block.

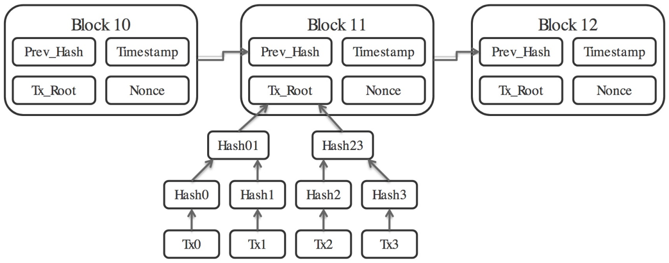


Fig. 1. Blocks are connected in a chained fashion where each block contains many transaction records. This figure is regenerated from [1].

Bitcoin miners collectively agree upon who receives the mined Bitcoins and which transactions to accept. This process of consensus, or agreement by majority, permanently records decisions in a public ledger called the blockchain. Bitcoin can be viewed as a large network of miners who compete in a lottery that awards newly mined currency, called Bitcoins, in exchange for contributing computational resources.

The blockchain supports a light-weight scripting language, designed to allow conditional transactions which can be re-purposed for other applications. Miners mine to fulfill two objectives: i) Correctly construct a new block and ii) Validate the transaction of each block.

A trustless and distributed consensus system means that if you want to send and/or receive money from someone you do not need to trust third-party services. If you use traditional methods of payment, you need to trust a third party to set your transaction (e.g. Visa, Mastercard, PayPal, banks). They keep their own private register which stores transactions history and balances of each account. With bitcoin and a few other digital currencies, everyone has a copy of the ledger (blockchain), no one has to trust third parties because anyone can directly verify the information written.

Adding a new record is very trivial in a centralized database system but it is time–consuming in a distributed database system like blockchain. In a centralized database system, all the records of a user are maintained centrally. Before adding a new record, it is easy to validate a new record after checking all the previous records of that user. In a centralized database system, it is easy to verify whether the user has enough money to complete the request. The validity of the request is easy to check. But in a distributed database system, in order to verify this request, we have to check the whole distributed database and compute the balance of that user. This step is time–consuming. After computing the balance, it is trivial to verify the request. Many methods are already established to compute this verification, two of them are: i) Proof–of–Work and ii) Proof–of–Stake.

We organized this paper as follows: in Section II, we discussed about Proof–of–Work. In Section III, we discussed about Proof–of–Stake method. A detailed analysis of blockchain is included in Section IV. In Section V, we discussed about an alternative method of blockchain called Tangle. Finally, in Section VI we conclude the paper.

II. Proof–of–Work

Proof–of–work (POW) method was invented by Cynthia Dwork and Moni Naor back in 1993. The term proof–of–work was coined by Markus Jakobsson and Ari Juels in a document published in 1999. In order to secure the transaction in a distributed database like block chain, Satoshi Nakamoto adopted this method in blockchain network.

This method deals with two parties, one is miner and the other one is verifier. Miners mine inside a block to find all the transactions belonging to that block. After mining all the transactions of a block, that block is ready to be added into the public blockchain and verifier can easily verify the transaction request. When a miner solves a block, it gains some reward in the form of bitcoin.

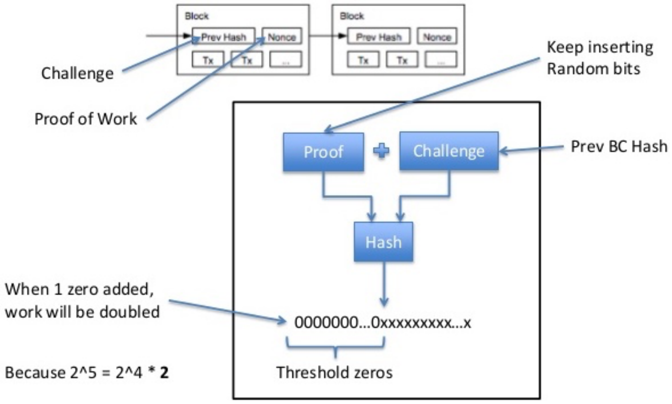


Fig. 2. Computational mechanism of Proof–Of–Work method. This figure is regenerated from [2].

Miners are general users who use their CPUs to solve a block. Each block contains many transactional history records. Supposing Alice wants to send $500 to Bob, how to verify that Alice has enough balance to send this amount of money to Bob becomes a question. To find the answer of this question, we need to dig into the distributed database and check each transaction which is related to Alice. Then, we need to accumulate all the transactions and do a simple calculation to find the current balance of Alice. The verifier can then easily verify the validity of this transaction.

In order to find the transaction histories of Alice, it is very inefficient to check all the transactions of a database. Each transaction in blockchain is hashed using SHA256 (some other hashing algorithms also used like scrypt, Blake–256, CryptoNight, HEFTY1, Quark, SHA–3, scrypt–jane, scrypt–n and combinations [3]). We use Alice's public key to check and filter out her transactions from the whole bunch of transactions. Searching Alice's transaction hash key using public key is similar to solving a puzzle. Searching appropriate hash key using public key is a brute–force method, which is time–consuming (see Fig. 2).

Fig. 3 shows the workflow of a proof–of–work mechanism. The loop part in the diagram is the most difficult part in computation. At each iteration, we need to increase the leading zero and compare the hash value with the exact hash value until the match occurs. Once one hash matches, the miner starts to unlock next puzzle. The miner who solves the entire block firstly gets rewarded and adds this block to the public block chain. Definitely, computationally faster miner will win and get rewarded.

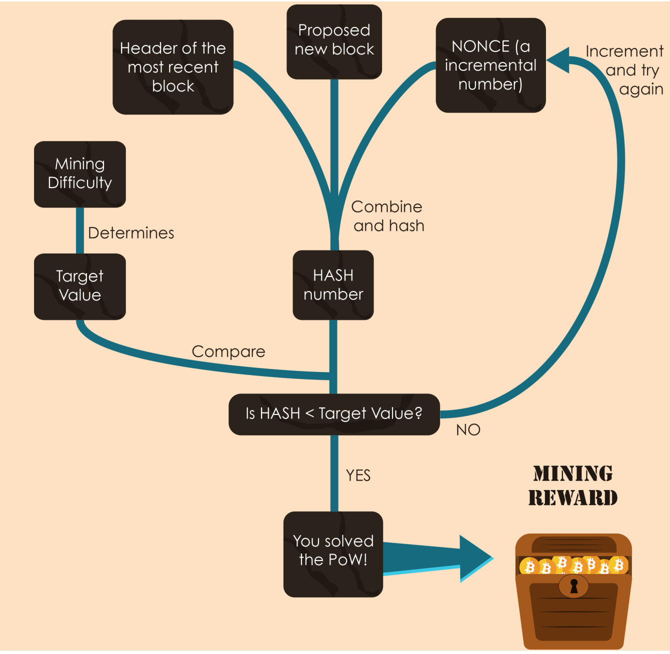


Fig. 3. Blocks are connected in a chained fashion where each block contains many transaction records. This figure is regenerated from [4].

Proof–of–work generates a product which is hard to construct and easy to verify. One of the most popular applications of this method is to create hashcash. This hashcash is used to verify email to prevent spam. It creates stamps to attach to mail to detect spamming. The main use of the hashcash stamp is as a white-listing hint to help users avoid losing emails due to content–based and blacklist–based anti–spam systems. It works with a cryptographic hash, such as SHA1, SHA256 or SHA3 which exhibits 2^{nd}–preimage resistance.

Pros:

- The computational hardness of this method imposes security. The block which needs more miners to solve is considered as more secure.

- It is verified with a single computation by checking that the SHA–1 hash of the stamp. So, it is fast and simple.

Cons:

1) Miners used their CPUs or GPUs or specific devices built for mining only and thus running these devices is energy-consuming.
2) The amount of reward that a miner gets after successfully completing the computation for a block is getting lower and after several years the reward will be just the transaction fee. The downgrade of the amount of reward will discourage miners from mining.
3) It is vulnerable for 51% attack. After controlling more than 50% of the mining hash rate, or computing power, the attackers would be able to prevent new transactions from gaining confirmations, and halt payments. They would also be able to reverse transactions, meaning they could double–spend coins.

In order to overcome this huge energy loss, block chain network provider is thinking about an alternate process named Proof–of–Stake.

III. Proof–of–Stake

As mentioned earlier, when a transaction is initiated, a block captures the transaction data. Later, data is duplicated across multiple nodes on the blockchain network. Every node can be a computer that uses its CPU/GPU power to solve a block, or it can be a computing device dedicated for solving hashcash. A miner, indicates a node in the network, uses its computing power to solve a computational power, which is known as Proof–of–Work problem. The first miner will get rewarded with coin. The solved block gets added to the blockchain, which is a public transparent ledger.

Proof–of–Stake (POS) is an alternative method of Proof–of–Work described above. According to this method, a miner or verifier can validate a block based on the amount of stake that verifier holds. That means, the more stake a miner holds can bring more mining power.

In Proof–of–Stake method, before starting solving a block, a group of miners agree to form a team and deposit coins as a stake. The large share means large stake and large portion of blocks to solve. When the block is mined then the reward amount is split based on the percentage of stakes each miner holds.

Fig. 4 shows how POS method works. Here, four validators mutually agreed to solve a block (showed at the middle). Initially based on agreement, they deposited coins to solve the block. The percentage of coins a validator deposited is called the stake of that validator. According to this figure, validator 1 holds the large portion of stake. During processing the block, after some random calculation, validator 1 has high probability to solve the entire block and gets rewarded. Fig. 5 shows that, validator 1 solves the entire block and gets rewarded by the transaction fee.

Pros:

- Proof–of–Stake method is more cost-effective.

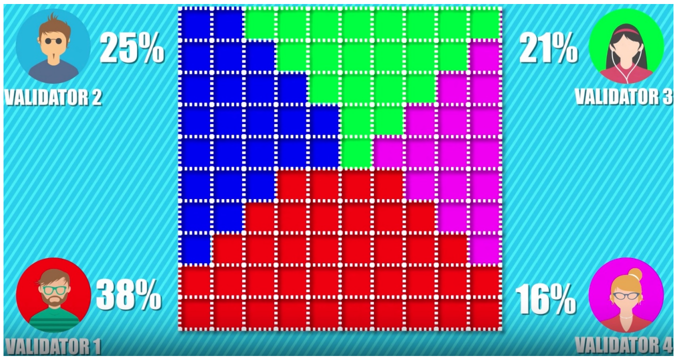


Fig. 4. Mechanism to distribute the blocks based on stake of four validators. This figure is regenerated from [5].

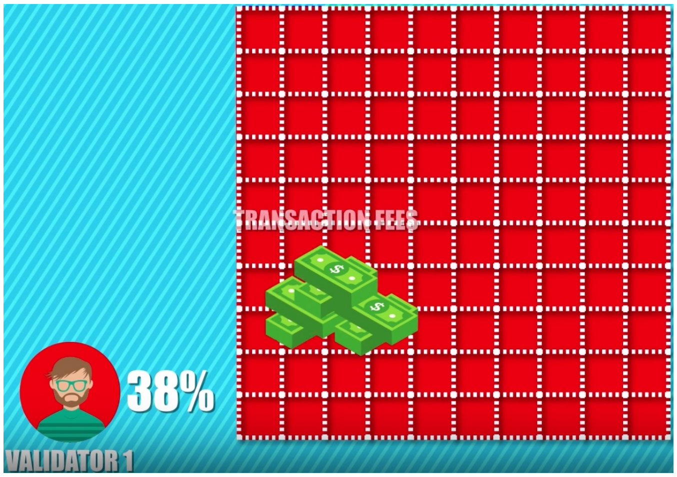


Fig. 5. Transaction fees as a form of reward given to the higher stake holder. This figure is regenerated from [5].

- It eliminates the burning; therefore, it is environmentally friendly.
- This method does not use any physical computational machine to solve puzzle, hence, it is an electric power saver mechanism.
- It is more secure. Like Proof–of–Work, if an attacker wants to do 51% attack then the attacker has to hold 51% of the total stake which is practically impossible.
- It solves cartels problem. Currently there are many blockchain pools. Each pool is a collection of nodes of blockchain network that is used to solve the puzzle problem. Fig. 6 shows the influence of a pool in the network using pie chart. The number of nodes under a pool is shown in a tabular form in Fig. 7. In PoS method, we do not need such pool system.
- As validators are depositing coins before solving a block and has chance to lose it, therefore, validators will not take risk of making the network vulnerable.
- Those "guarding" the coins are always those who own the coins though several cryptocurrencies do allow or enforce lending the staking power to other nodes.

Cons:

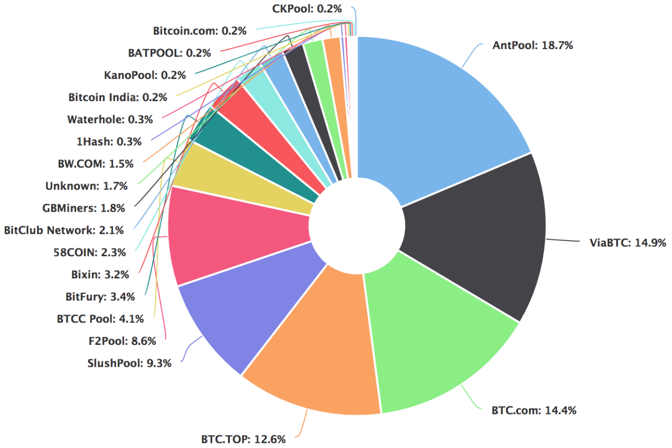


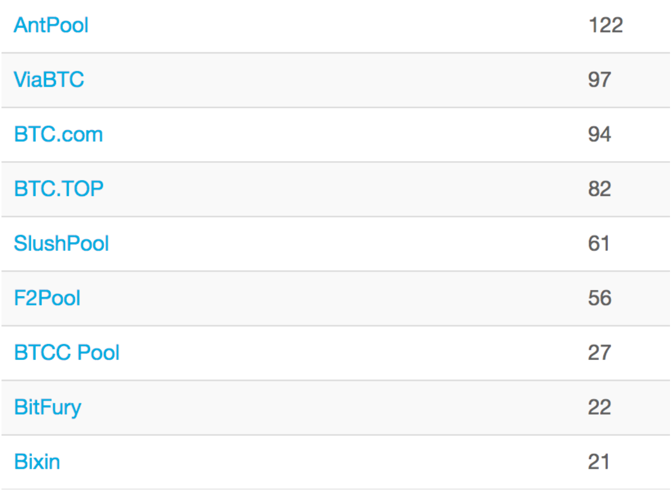
Fig. 6. The pie chart shows different pools and the percentage shows the coverage of the network. This figure is regenerated from [6].

1) The higher stake holder has high probability to solve a block and get the reward. Hence, the rich will get richer.
2) In Proof–of–work method, the miner needs to buy ASICs or other computing devices that make a bigger contribution in economy. When the miner does not get rewarded then he/she can feel the loss but in Proof–of–stake method, the miner has nothing to lose in terms of physical cash. Hence, the miner will try to solve every block.
3) It has initial distribution problem, which is how to distribute the coins initially because the reward goes to the stake holders.
4) Long range attack can occur in blockchain.
5) Coinage accumulation attack can occur.
6) Pre-computing attack can occur.
7) There is the "nothing at stake" problem, that block–generators have nothing to lose by voting for multiple blockchain–histories, which prevents the consensus from ever resolving. Because there is little cost in working on several chains, anyone can abuse this problem to attempt to double–spend (in case of blockchain reorganization) "for free".

IV. Analysis

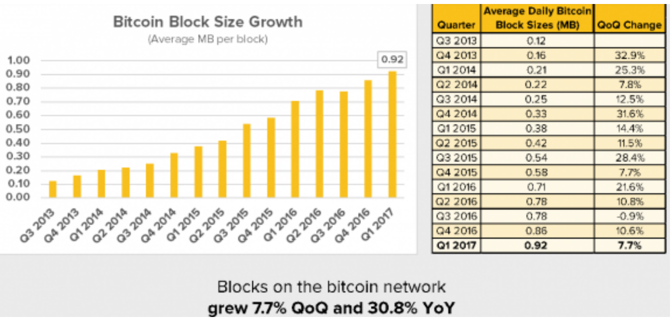
Blockchain is a revolutionary mechanism that ensures secure distributed storage of data. This mechanism diminishes the concept of trusted third party. Each node of blockchain network holds information of everyone but only the data owner can access his/her data using private key. If private key is lost somehow then the corresponding data will be lost in the way that user can't retrieve the data anyway. Hence, necessity of remembering the private key is one of the drawbacks of this mechanism.

Bitcoin transaction is now getting popular day by day. Fig. 8 shows the popularity of bitcoin in the form of the size of block. The block size continues to grow as the amount of transaction increases. According to the chart, 92% of a block is already occupied this year.



AntPool	122
ViaBTC	97
BTC.com	94
BTC.TOP	82
SlushPool	61
F2Pool	56
BTCC Pool	27
BitFury	22
Bixin	21

Fig. 7. The list shows the name of the pool and the number of nodes of the network working to mine puzzle. We see that first 4 pools cover almost 60% of the total network nodes. This figure is regenerated from [6].



Quarter	Average Daily Bitcoin Block Sizes (MB)	QoQ Change
Q3 2013	0.12	
Q4 2013	0.16	32.9%
Q1 2014	0.21	25.3%
Q2 2014	0.22	7.8%
Q3 2014	0.25	12.5%
Q4 2014	0.33	31.6%
Q1 2015	0.38	14.4%
Q2 2015	0.42	11.5%
Q3 2015	0.54	28.4%
Q4 2015	0.58	7.7%
Q1 2016	0.71	21.6%
Q2 2016	0.78	10.8%
Q3 2016	0.78	-0.9%
Q4 2016	0.86	10.6%
Q1 2017	**0.92**	**7.7%**

Blocks on the bitcoin network
grew 7.7% QoQ and 30.8% YoY

Fig. 8. Bitcoin block size is growing faster year to year. This figure is regenerated from [7].

Bitcoin is the most successful application case of blockchain, but it can be used for other purposes too. Ethereum is trying to make the blockchain network flexible to use for any distributed storage. Now we can use blockchain to make and store smart contract. Blockchain can be used to store the information for IoT devices. There are many other applications, such as Blockfolio, Coin Tracking, Lawnmower, Ztrader, Google Authenticator, etc.

Bitcoin miners' reward (coins) is getting higher from month to month. Fig. 9 shows that over the time, the monthly miner fee rises up to 35–fold. It is nearly 12–fold increase if we increase the transaction growth by nearly 3 times [8]. According to the chart, the fee is rising exponentially, which leads us to the equilibrium situation when the most powerful computing network makes the transaction secure with the true value of fees.

Although the popularity of blockchain is growing fast day by day, it contains some limitations as follows:

Regulation: Regulation controls the adaptability of an industry and it is critical to realize how regulatory institutions will react to blockchain technology. Some countries or states are able to form a regulatory environment for this technology.

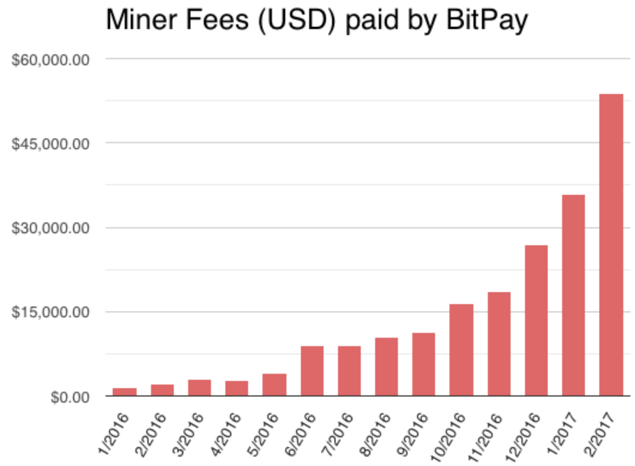


Fig. 9. Miner's fee is getting higher from month to month. This figure is regenerated from [8].

The security feature of this technology is much more attractive even though there are many queries on this technology which needs time to be answered.

Scalability: The amount of transaction using blockchain technology is very discrete. Fig. 10 shows the comparison of transaction rate among Bitcoin, Ethereum, Paypal, and Visa. According to this chart, there still has a lot of work to be done in order to reduce the difference.

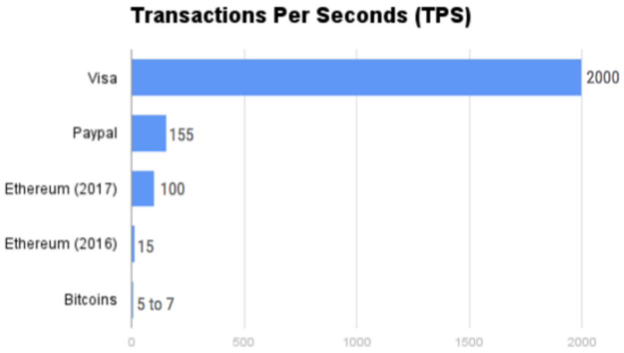


Fig. 10. The chart shows the variation of the transaction per second rate for different payment methods. This figure is regenerated from [9].

Privacy: Blockchain is a public ledger. Privacy is important in blockchain because everyone has access to all the information stored in a blockchain. There are some cryptographic techniques developed to store encrypted data in blockchain. Currently it is not possible to make the real data visible to a certain type of user which is possible in a centralized system.

Storage: The block capacity in a blockchain currently is $1MB$ which is very small and cannot store $3MB$ sized pdf. In order to store more information blockchain system needs a way to link with a storage system.

Standards: The connection is missing between blockchain and other existing technology in a certain or standard way. There should be a connection framework that embeds blockchain technology to other technologies without creating a new type of blockchain technology.

Industry Consensus: It is hard to change the structure of an industry where they will not have any control over the server or the infrastructure.

Computational security: Currently blockchain used Proof–of–Work consensus because it is computationally hard and this hardness imposes indirect security over the network. In the near future when quantum computers are developed, then blockchain will fall in a real threat because a quantum computer is 17 billion times more efficient at mining the Bitcoin blockchain than a classical computer [10].

To mitigate this future threat on blockchain *Serguei Popov* proposed an alternative of blockchain, which is called *Tangle*. *IOTA*, a cryptocurrency for the Internet-of-Things (IoT) industry applications Tangle as a backbone described in next section.

V. IOTA

IOTA is an alternative of Bitcoin and it used Tangle as a distributed ledger instead of Blockchain. Fig. 11 shows the structure of the tangle network. The network is a directed acyclic graph where each node indicates an entity that issues and validates transaction [10]. The edge indicates the relationship between a new transaction and the old transaction. The direction of an edge is from a new transaction to one of the recent transactions. In order to approve a new transaction, Tangle verifies most recent two transactions, hence, each node points to at most two previous nodes in terms of time.

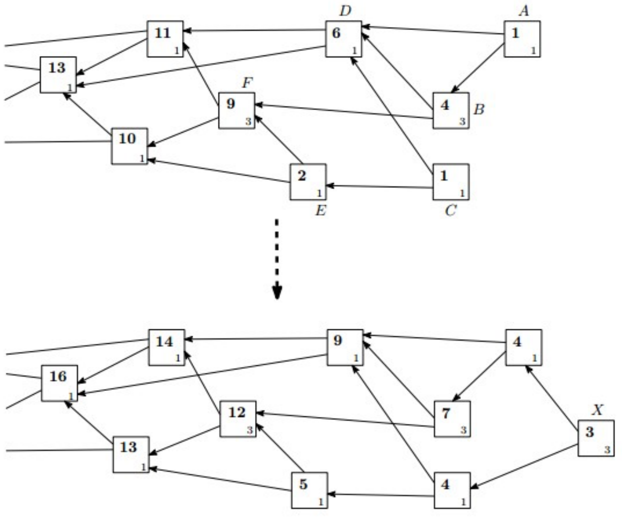


Fig. 11. The network architecture of tangle. Each node is an entity that issues and validates transactions. The nodes are growing from left to right according to the growth of time. This figure is regenerated from [10].

Each node contains information of two weights, one is its own weight (bottom–right corner) and the other one is the cumulative weight (at center). The cumulative weight of a node is the summation of all the node weights along the path that ends at that node. According to Fig. 11, two paths ended at node F, where one path contains node A and node B and the other path contains node C and node F. The cumulative weight of F is $\sum_{s\in\{A,B,C,D,F\}}\omega(s) = 1+3+1+1+3 = 9$. The weight feature prevents Tangle from a quantum computer attack [10].

Pros:

1) This system does not require any transaction fee, hence, users can send micropayment, which is not possible in blockchain technology.
2) There is no concept of miner, everyone contributes to the network.
3) Unlimited scalability.
4) Network remains as it is, it does not split into many fragments like ETH and ETC.
5) The idea is based on a machine–to–machine ($M2M$) payment, in which technical devices autonomously shift money among themselves. IOTA is therefore primarily aimed at machines instead of people.

Cons:

- Building smart contract is not possible.
- The method to free transaction fee is not practical. Heavy weighted DAG could force transactions through themselves and charge fees [11].
- In order to attack on the network, the attacker does not have to waste enough computational power.
- We know that ternary processors are theoretically more efficient than binary processors. IOTA is by necessity built to run on existing hardware, which is exclusively binary. As a result, all of its internal ternary notation has to be encapsulated in binary, resulting in significant storage and computational overhead.
- The theoretical benefits of a balanced ternary notation, such as not needing a sign bit, are more than outweighed by the practical disadvantages, because every processor on which IOTA will run is already equipped to perform math on twos–complement numbers, but requires software emulation to operate on balanced ternary.

VI. Conclusion

Digital cryptocurrency starts to make influence in global economy and gradually makes people get accustomed to it. Blockchain plays an important role to make the transaction secure and reliable. The proof–of–work mechanism makes the transaction rate slow compared to other centralized transaction systems like VISA, Paypal, etc. Blockchain opens the opportunity of data storage, management and security on IoT devices. Even though we can’t store enough amount of data but it successfully turns to be real. Besides, IOTA opens a more flexible and secure door in the world of cryptocurrency and this field is maturing day by day with the enormous contributions of scholars.

References

[1] “blockchain diagram,” https://upload.wikimedia.org/wikipedia/commons/5/55/Bitcoin_Block_Data.svg, [Last; accessed December-11].

[2] “Hybrid blockchain,” https://steemit.com/cryptocurrency/@rrrenaldooo/what-is-hybrid-blockchain-proof-of-work-and-proof-of-stake-explained, [Last; accessed December-11].

[3] “What is proof of work,” https://www.bitcoinmining.com/what-is-proof-of-work/, [Last; accessed December-11].

[4] “Proof-of-work diagram,” https://www.bitcoinmining.com/images/what-is-proof-of-work-high-resolution.png, [Last; accessed December-11].

[5] “Proof of work vs proof of stake - simplified explanation,” https://www.youtube.com/watch?v=SiKnWBPkQ4I, [Last; accessed December-11].

[6] “Blockchain pools,” https://blockchain.info/pools, [Last; accessed December-11].

[7] “Bitcoin block size,” https://media.coindesk.com/uploads/2017/06/Blocks-728x410.png, [Last; accessed December-11].

[8] “The bitcoin fee market,” https://medium.com/@spair/the-bitcoin-fee-market-4df1857d12b7, [Last; accessed December-11].

[9] “Roadblocks of blockchain,” https://stayrelevant.globant.com/en/roadblocks-of-blockchain/, [Last; accessed December-11].

[10] S. Popov, “The tangle,” *cit. on*, p. 131, 2016.

[11] “Iota: Is it worth one iota?” https://steemit.com/iota/@wolfofcrypto/iota-is-it-worth-one-iota, [Last; accessed December-11].